EY Fraud Investigation & Dispute Services

Managing insider threat through the lens of a seasoned investigator

August 2017

Building a better working world

Louis Bladel, Executive Director

Contact Information
1101 New York Avenue,
Washington, DC 20005

Office: + 1 202 327 7426
Mobile: + 202 359 8172
Lou.bladel@ey.com

Education
BS, Criminal Justice Sciences,
Illinois State University

Memberships
President of the board of trustees, the Kingsbury Day School
Illinois State University's College of Applied Science and Technology of Hall of Fame for career achievement
Intelligence & National Security Alliance (INSA)
FBI Domestic Security Alliance Council
FBI's Agent Association

- Lou Bladel is an ***Executive Director in the Fraud Investigations & Dispute Services practice*** of Ernst & Young, LLP. He is the *National Coordinator for Insider Risk and Threat Management services,* which assists clients in responding to, investigating and remediating insider threats, as well as developing and implementing comprehensive insider threat programs and services. Lou consults with U.S. federal law enforcement agency directors, government regulators and key executives of Fortune 100 companies, Fortune 500 C-suite officials and boards of directors from across industry sectors on matters of economic espionage and insider threats.

- Lou has ***more than 26 years of federal law enforcement experience serving in the U.S. Marshals Service, Naval Criminal Investigative Service and a Special Agent of the Federal Bureau of Investigation (FBI),*** retiring from the FBI in 2016. The majority of Lou's law enforcement career involved leading and investigating counterintelligence matters in the New York and Washington, DC, metropolitan areas. Lou has held numerous leadership positions within the FBI, including **Special Agent-in-Charge of the New York office of the FBI's Counterintelligence Division**, where he led the recent espionage/insider threat arrest and successful plea negotiations of an FBI employee.

- ***As Chief of the FBI's Counterespionage Section, he led the espionage investigations of General David Petraeus and Edward Snowden.*** In 2013, he successfully testified before the U.S. Sentencing Commission to enhance the criminal penalties for theft of propriety information and managed the DuPont economic espionage investigation, which resulted in the FBI's first-ever jury conviction for economic espionage. The case won the **2014 FBI Director's Award for Counterintelligence Excellence**. Lou also won the National Counterintelligence Executive Award for Community Excellence in leadership for his role in the FBI operation that led to the arrest and deportation of three Russian Intelligence Service illegals.

Agenda

- Case studies
  - Edward Snowden
  - DuPont Investigation
  - Kun Shan“Joey” Chun
- Takeaways & lessons learned from each case study
- Key steps for building an Insider Threat Program

Case studies

Edward Snowden
Chronological events

- High school dropout
- 2004: Enlisted in US Army Reserve as special forces recruit in May; discharged in September without completing training
- 2005: Hired by NSA as a security guard
- 2006: Hired by CIA as an IT system administrator
- 2009: Hired by Dell as an NSA subcontractor
- April 2013: Hired by BAH as a senior consultant and became a system administrator at an NSA facility in Hawaii
- Jan – May 2013: Initiated a number of contacts with the media using alias “Verax” and encrypted communications (e.g., filmmaker, Laura Poitras, Glenn Greenwald @*the Guardian,* Barton Gellman @*the Washington Post).*

Edward Snowden
Chronological events

- June 1, 2013: Greenwald and Poitras interviewed Snowdon in Hong Kong
- June 5 - 9, 2013: First story published in UK Guardian; Snowden voluntarily revealed his identity in UK Guardian
- June 14, 2013: Charged in EDVA with violation of Title 18 USC
- June 15 - 23, 2013: Provisional arrest request made to HKSAR authorities; Snowden's US passport revoked; Snowden departed Hong Kong for Moscow
- August 1, 2013: Snowden granted political asylum in Russia for one year.
- January, 2014: Russia announced that Snowden can stay in country "indefinitely"

Edward Snowden
Key takeaways

- NSA was considered in 2013 to be the “security gold standard” and failed
- Perfect storm of arrogance, lack of understanding of vulnerabilities, and unwillingness to question inappropriate activities
- Leadership did not take insider threat seriously
- Focused on what most consider to be “cybersecurity,” i.e., perimeter security, or securing the facility against threats from outsiders
- Failed to implement a repeatable, holistic program

DuPont investigation

Walter Liew

Naturalized US citizen

Owner and executive of USA Performance Tech Inc. (USAPTI)

Sentence: 15 years plus $27 million fine

Christina Liew

Naturalized US citizen

Owner and executive of USAPTI; wife of Walter Liew

Sentence: 3 years of probation plus $6 million fine

Robert Maegerie

US citizen

DuPont engineer (1956–991)

Sentence: 30 months plus $375,000 fine

Tze Chao

Naturalized US citizen

Former DuPont scientist (1966–2002)

Sentence: 15 years in prison

DuPont investigation key takeaways

- Inadequate understanding of the threat to its intellectual property
- Insufficient measures to secure trade secrets
- Limited pre- and post-employment checks and security protocols
- Failed to detect and respond to the breach in time

Kun Shan “Joey” Chun
Chronological events

- Born in Guandong, China, in 1969; naturalized American citizen in 1985
- 1997: Hired as an FBI electronics technician
- 1998: Granted a top secret clearance with access to classified information of FBI and other government agencies
- 2006: Recruited by the Chinese Ministry of State Security (MSS) and became a consultant to a Chinese company in exchange for financial benefits
- 2014: FBI became aware of Kun Shan Chun’s activities. Chun attempted to recruit a FBI undercover employee (UCE) on behalf of the Chinese MSS and expressed to UCE desire to pass USG information to the Chinese Government.
- March 2016: Arrested and charged in SDNY with violation of Title 18 USC:
- August 2016: Pleaded guilty to § Sec. 951(a)

Kun Shan “Joey” Chun
Key takeaways

- FBI didn’t have formalized training of insider threat protocols pushed out to the operational divisions. (FBI instituted new insider threat protocols in Spring 2014.)
- Chun’s immediate supervisors failed to recognize unusual travel patterns and irregularities in spending patterns.

Building an insider threat program

Key steps for building an insider threat program

- Gain senior leadership endorsement, develop policies that have buy-in from key stakeholders and take into account organizational culture
- Develop repeatable processes to achieve consistency in how insider threats are monitored and mitigated
- Use analytics to strengthen the program backbone, but remember implementing an analytical platform does not create an insider threat detection program in and of itself
- Coordinate with legal counsel early and often to address privacy, data, protection and cross-border data transfer concerns

Key steps for building an insider threat program

- Screen employees and vendors regularly, especially personnel who hold high-risk positions or have access to critical assets
- Implement clearly defined consequence management processes so that all incidents are handled following consistent standards, involving the right stakeholders
- Create training curriculum to generate awareness about insider threats and their related risks
- Leverage information security and corporate security programs, coupled with information governance, to identify and understand critical assets

A brief introduction to managing insider threat

Questions?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With over 4,500 fraud investigation and dispute professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

© 2017 EYGM Limited.
All Rights Reserved.

1701-2161236
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com